16869Y-108700 US

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１１月１９日

出願番号
Application Number: 特願２００３－３８９４７５

[ST. 10/C]: [ＪＰ２００３－３８９４７５]

出願人
Applicant(s): 株式会社日立製作所

２００４年 ２月１７日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００４－３００９９７７

【書類名】　特許願
【整理番号】　HK15230000
【提出日】　平成15年11月19日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 12/00
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
　【氏名】　古川　博
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
　【氏名】　赤川　悦太郎
【特許出願人】
　【識別番号】　000005108
　【氏名又は名称】　株式会社　日立製作所
【代理人】
　【識別番号】　110000198
　【氏名又は名称】　特許業務法人湘洋内外特許事務所
　【代表者】　三品　岩男
　【電話番号】　045(316)3711
【手数料の表示】
　【予納台帳番号】　221535
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
ホスト計算機と通信回線を介して接続される記憶装置であって、
前記通信回線に接続するためのインタフェースを備え、
前記インタフェースは、前記通信回線から通信パケットを受信した際、当該通信パケットの中から前記記憶装置へのアクセス用として予め定められたフォーマットの通信パケットであるか否かを判別する第一のフィルタ手段を備えること
を特徴とする記憶装置。
【請求項２】
請求項１記載の記憶装置であって、
前記インタフェースは、前記第一のフィルタ手段において、前記アクセス用と判別された前記通信パケットを受け取り、前記記憶装置内の記憶領域へのアクセスが許可された前記ホスト計算機から送信された通信パケットであるか否かを判別する第二のフィルタ手段をさらに備えること
を特徴とする記憶装置。
【請求項３】
請求項２記載の記憶装置であって、
前記インタフェースは、前記ホスト計算機が前記記憶装置にアクセスが許可されている場合、当該ホスト計算機を一意に特定する情報と、当該ホスト計算機がアクセスを許可されている前記記憶装置内の記憶領域を特定する情報と、を備えたアクセス許可テーブルをさらに備え、
前記第二のフィルタ手段は、前記アクセス許可テーブルに格納された情報に従い、前記アクセス用と判別された通信パケットが、アクセスが許可されたホスト計算機から送信されたものであるか否かを判別すること
を特徴とする記憶装置。
【請求項４】
請求項１、２、および、３いずれか一項記載の記憶装置であって、
前記インタフェースは、
当該インタフェースにおいて受信した全ての通信パケットの通信量と、前記第一のフィルタ手段において前記フォーマットの通信パケットでないものと判定された通信パケットの通信量とをそれぞれ測定し、両通信量を用いて、通信障害が発生しているか否かを判定する通信障害判定手段と、
前記通信障害判定手段において、通信障害が発生していると判断された場合、当該記憶装置に接続され、通知を受けた情報を表示する機能を備える管理サーバに通知する通信障害通知手段とをさらに備えること
を特徴とする記憶装置。
【請求項５】
請求項４記載の記憶装置であって、
前記通信障害判定手段は、前記第二のフィルタ手段において前記アクセスが許可されたホスト計算機から送信された通信パケットでないと判別された通信パケットの通信量をさらに測定し、当該通信量と前記全ての通信パケットの通信量とを用いて、通信障害が発生しているか否かを、さらに判定すること
を特徴とする記憶装置。
【請求項６】
請求項５に記載の記憶装置であって、
前記インタフェースは、
前記第一のフィルタ手段において前記フォーマットの通信パケットでないものと判別された通信パケットおよび前記前記第二のフィルタで前記アクセスが許可されたホスト計算機から送信された通信パケットでないと判別された通信パケットの通信情報を、通信ログとして記録する通信ログ記録手段をさらに備えること

を特徴とする記憶装置。

【請求項７】

請求項４～６いずれか一項記載の記憶装置に接続された管理サーバであって、

前記記憶装置の通信障害通知手段から通信障害が発生していると通知を受けた場合、前記通信ログを参照し、通信障害を発生させている前記通信パケットの発信元を抽出する発信元抽出手段を備えること

を特徴とする管理サーバ。

【請求項８】

請求項７記載の管理サーバであって、

前記発信元抽出手段で抽出された発信元の情報を元に、当該発信元からの通信を遮断するよう前記通信回線上に備えられた前記記憶装置への通信を中継する中継装置を制御する中継装置制御手段をさらに備えること

を特徴とする管理サーバ。

【請求項９】

ホスト計算機と通信回線を介して接続される記憶装置に搭載されるコンピュータを、

前記通信回線に接続するためのインタフェース手段と、

前記通信回線から前記インタフェース手段を介して通信パケットを受信した際、当該通信パケットの中から前記記憶装置へのアクセス用として予め定められたフォーマットの通信パケットであるか否かを判別する第一のフィルタ手段と

して機能させるためのプログラム。

【請求項１０】

ホスト計算機と通信回線を介して接続される記憶装置に搭載されるコンピュータを、

前記通信回線に接続するためのインタフェース手段と、

前記通信回線から前記インタフェース手段を介して通信パケットを受信した際、当該通信パケットの中から前記記憶装置へのアクセス用として予め定められたフォーマットの通信パケットであるか否かを判別する第一のフィルタ手段と、

前記第一のフィルタ手段において、前記アクセス用と判別された前記通信パケットを受け取り、前記記憶装置内の記憶領域へのアクセスが許可された前記ホスト計算機から送信された通信パケットであるか否かを判別する第二のフィルタ手段と

して機能させるためのプログラム。

【請求項１１】

ホスト計算機と通信回線を介して接続される記憶装置に搭載されるコンピュータを、

前記通信回線に接続するためのインタフェース手段と、

前記通信回線から前記インタフェース手段を介して通信パケットを受信した際、当該通信パケットの中から前記記憶装置へのアクセス用として予め定められたフォーマットの通信パケットであるか否かを判別する第一のフィルタ手段と、

前記インタフェース手段において受信した全ての通信パケットの通信量と、前記第一のフィルタ手段において前記フォーマットの通信パケットでないものと判別された通信パケットの通信量とをそれぞれ測定し、両通信量を用いて、通信障害が発生しているか否かを判定する通信障害判定手段と、

前記通信障害判定手段において、通信障害が発生していると判断された場合、当該記憶装置に接続され、通知を受けた情報を表示する機能を備える管理サーバに通知する通信障害通知手段と、

して機能させるためのプログラム。

【請求項１２】

記憶装置と接続される管理サーバに搭載されるコンピュータを、

前記記憶装置から通信障害が発生していることを示す通知を受けた場合、当該記憶装置が保持する通信ログを参照し、前記通信障害を発生させている通信パケットの発信元を抽出する発信元抽出手段と

して機能させるためのプログラム。

【請求項１３】
記憶装置と接続される管理サーバに搭載されるコンピュータを、
前記記憶装置から通信障害が発生していることを示す通知を受けた場合、当該記憶装置が保持する通信ログを参照し、前記通信障害を発生させている通信パケットの発信元を抽出する発信元抽出手段と、
前記発信元抽出手段で抽出された発信元の情報を元に、当該発信元からの通信を遮断するよう、前記記憶装置が通信パケットを受け取るために接続されている通信回線上に備えられた前記記憶装置への通信を中継する中継装置を制御する中継装置制御手段と
して機能させるためのプログラム。
【請求項１４】
請求項９～１３いずれか一項記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項１５】
記憶装置とホスト計算機と管理サーバとが通信回線により接続される記憶装置システムであって、
前記記憶装置は、前記通信回線に接続するためのインタフェースを備え、
前記インタフェースは、
前記通信回線から通信パケットを受信した際、当該通信パケットの中から前記記憶装置へのアクセス用として予め定められたフォーマットの通信パケットであるか否かを判別する第一のフィルタ手段と、
前記第一のフィルタ手段において、前記アクセス用と判別された前記通信パケットを受け取り、前記記憶装置内の記憶領域へのアクセスが許可された前記ホスト計算機から送信された通信パケットであるか否かを判別する第二のフィルタ手段と、
当該インタフェースにおいて受信した全ての通信パケットの通信量および前記第一のフィルタ手段において前記フォーマットの通信パケットでないものと判定された通信パケットの通信量をそれぞれ測定し、両通信量を用いて、通信障害が発生しているか否かを判定する通信障害判定手段と、
前記通信障害判定手段において、通信障害が発生していると判断された場合、前記管理サーバに通知する通信障害通知手段と、
前記第一のフィルタ手段において前記フォーマットの通信パケットでないものと判定された通信パケットおよび前記第二のフィルタ手段において前記アクセスが許可された前記ホスト計算機から送信された通信パケットでないものと判別された通信パケットの通信ログを記録する通信ログ記録手段と、
を備え、
前記管理サーバは、
前記通信障害通知手段から受けた通知を表示する表示手段と、
前記通信障害通知手段から通信障害が発生していると通知を受けた場合、前記通信ログを参照し、通信障害を発生させている前記通信パケットの発信元を抽出する発信元抽出手段と、
前記発信元抽出手段で抽出された発信元の情報を元に、当該発信元からの通信を遮断するよう前記通信回線上に備えられた前記記憶装置への通信を中継する中継装置を制御する中継装置制御手段と、を備えること
を特徴とする記憶装置システム。
【請求項１６】
請求項１５記載の記憶装置システムであって、
前記インタフェースは、前記ホスト計算機が前記記憶装置にアクセスが許可されている場合、当該ホスト計算機を一意に特定する情報と、当該ホスト計算機がアクセスを許可されている前記記憶装置内の記憶領域を特定する情報と、を備えたアクセス許可テーブルをさらに備え、
前記第二のフィルタは、前記アクセス許可テーブルに格納された情報に従い、前記アク

セス用と判別された通信パケットが、アクセスが許可されたホスト計算機から送信されたものであるか否かを判別すること
を特徴とする記憶装置システム。
【請求項１７】
請求項１５または１６記載の記憶装置システムであって、
前記通信障害判定手段は、前記第二のフィルタ手段において前記アクセスが許可された前記ホスト計算機から送信された通信パケットでないと判別された通信パケットの通信量をさらに測定し、当該通信量と前記全ての通信パケットの通信量とを用いて、通信障害が発生しているか否かを、さらに判定すること
を特徴とする記憶装置システム。
【請求項１８】
請求項１７記載の記憶装置システムであって、
前記通信障害判定手段は、前記第二のフィルタ手段において前記アクセスが許可された前記ホスト計算機から送信された通信パケットと判別された通信パケットの通信量をさらに測定し、当該通信量と前記全ての通信パケットの通信量とを用いて、前記アクセスが許可されたホスト計算機から送信された通信パケットの通信量の全通信パケットの通信量に対する比の値が所定以下であるか否かを判別し、
前記通信障害通知手段は、前記通信障害判定手段において、当該比の値が所定以下と判別された場合、第二の通信障害が発生していることを示す通知を前記管理サーバに通知し、
前記管理サーバは、
前記通信障害通知手段から第二の通信障害が発生していることを示す通知を受けた場合、予め管理者により設定されている前期記憶装置と前記ホスト計算機との間の通信帯域を再調整する帯域調整手段、をさらに備えること
を特徴とする記憶装置システム。
【請求項１９】
記憶装置とホスト計算機と管理サーバとが通信回線により接続される記憶装置システムにおける通信制御方法であって、
前記記憶装置が通信回線からの通信パケットを受信した際、当該通信パケットの中から前記記憶装置へのアクセス用として予め定められたフォーマットの通信パケットであるか否かを判別する第一のフィルタリングステップと、
前記記憶装置が受信した全ての通信パケットの通信量および前記第一のフィルタリングステップにおいて前記フォーマットの通信パケットでないと判別された通信パケットの通信量をそれぞれ測定し、両通信量を用いて、通信障害が発生しているか否かを判定するとともに、前記第一のフィルタリングステップにおいて前記フォーマットの通信パケットでないと判別された通信パケットの通信ログを記録する通信障害判定ステップと、
前記通信障害判定ステップにおいて、通信障害が発生していると判断された場合、前記管理サーバに通知する通信障害通知ステップと、
前記記憶装置から通信障害が発生していると通知を受けた場合、前記通信ログを参照し、当該通信障害を発生させている前記通信パケットの発信元を抽出する発信元抽出ステップと、
前記発信元抽出ステップで抽出された発信元の情報を元に、当該発信元からの通信を遮断するよう前記通信回線上に備えられた前記記憶装置への通信を中継する中継装置を制御する中継装置制御ステップと、を備えること
を特徴とする通信制御方法。

【書類名】明細書
【発明の名称】記憶装置、記憶装置システム、および、通信制御方法
【技術分野】
【０００１】
本発明は、ホスト計算機と記憶装置との間の通信に関する。特に、前記ホスト計算機から前記記憶装置内の論理ユニットへのアクセス時の通信におけるフィルタリング技術および通信遮断技術に関する。
【背景技術】
【０００２】
1以上のホスト計算機と1以上の記憶装置とをネットワークで接続したストレージシステムにおいて、ホスト計算機から記憶装置内の論理ユニットＬＵ（Ｌｏｇｉｃａｌ　Ｕｎｉｔ）へアクセスする際の不正アクセスを防止するセキュリティ技術がある。一例として、ホスト計算機毎にアクセス可能な論理ユニットを制限している環境において、発信元のホスト計算機に関する情報によって受け取った情報のアクセス可否を判断するフィルタリング機能を記憶装置側に備えることで不正なアクセスの遮断を実現しているものがある（例えば、特許文献１参照。）。
【０００３】
特許文献１に開示されているストレージシステムは、記憶装置内の不揮発メモリ上に、ホスト計算機を一意に識別する情報であるＷＷＮ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｎａｍｅ）と、前記ホスト計算機からのアクセスを許可した記憶装置内の論理ユニットの番号であるＬＵＮ（Ｌｏｇｉｃａｌ　Ｕｎｉｔ　Ｎｕｍｂｅｒ）と、前記ＬＵＮに対応してユーザやホスト計算機上のオペレーティングシステムが任意に割当てた仮想的なＬＵの番号である仮想ＬＵＮとを対応づけて管理するＬＵＮアクセス管理テーブルに加え、前記ホスト計算機が前記記憶装置にアクセスする際の通信において、ログイン時に動的に割当てられ、前記ホスト計算機が稼働している間は常に一定である管理番号であるＳ－ＩＤ（Ｓｏｕｒｃｅ　ＩＤ）と、前記ホスト計算機のＷＷＮとを対応づけて管理するＷＷＮ－Ｓ－ＩＤ管理テーブルを持つ。
【０００４】
特許文献1に開示されているストレージシステムでは、これらの２つの管理テーブルを参照することにより、論理ユニットに対するアクセスの可否を、ログイン時の問合せコマンド発生時点で判断し、以後、この判定を繰り返す必要がない。このため、記憶装置を高い性能で維持運用しながら、論理ユニット単位でアクセス可否を制限でき、強固なセキュリティを実現している。
【０００５】
ただし、特許文献１に開示されているストレージシステムは、ファイバチャネル（Ｆｉｂｒｅ　Ｃｈａｎｎｅｌ；ＦＣ）という専用のインタフェースを用いてホスト計算機と記憶装置とを接続してネットワーク化したＳＡＮ（Ｓｔｏｒａｇｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）などの、専用ネットワークにより構築されたシステムである。このため、記憶装置へは、ホスト計算機から記憶装置へのアクセス用のコマンドセットであるＳＣＳＩコマンドのみが送信されてくることが前提である。
【０００６】
一方、近年、ＳＣＳＩコマンドを、ＩＰネットワーク上で送受信するためのプロトコルであるｉＳＣＳＩの標準仕様が、標準化団体ＩＥＴＦにて検討されている。
【０００７】
ｉＳＣＳＩでは、ＳＣＳＩコマンド等を、ＩＰパケットのペイロードに格納されているＴＣＰパケットの伝送フレームの中に格納（カプセル化）してＩＰネットワーク上を流すことにより、コマンドの送受を行い、ホスト計算機と記憶装置との間のＩ／Ｏ処理を実現する。
【０００８】
ｉＳＣＳＩを用いることにより、ホスト計算機だけでなく記憶装置も直接ＩＰネットワ

ークに直結でき、従来からＩＰネットワークで用いられていた、ネットワーク網を構築するハブやルータ、スイッチ類などもそのまま使用できる。

【０００９】

従って、ＩＰネットワークを利用して、これまでコスト面や通信距離限界といった技術面から実現が難しかった記憶装置アクセスの広域化に容易に対応できるとともに、成熟しているＩＰネットワーク管理技術がそのまま適用でき、管理の簡素化も期待できる。

【００１０】

【特許文献１】特開２００１－２６５６５５号公報

【発明の開示】

【発明が解決しようとする課題】

【００１１】

しかしながら、前記のｉＳＣＳＩには、上述のようなメリットがある反面、デメリットも存在する。

【００１２】

ＩＰネットワーク上では、多種多様な通信パケットが送受信されている。このため、これまでのホスト計算機と記憶装置との間の専用ネットワークであるＦＣネットワークで接続されていた場合に比べ、トラフィック通信性能などを予測できない面がある。

【００１３】

また、ＩＰネットワークは、全世界に張り巡らされているため、悪意を持った利用者が、ＩＰネットワークに接続された記憶装置等を対象に、システムダウン、データ改竄、窃盗などを目的とした通信攻撃を仕掛けてくる可能性もあり、セキュリティ面で脆弱性を抱えている。

【００１４】

特許文献１に開示されているフィルタリング機能は、記憶装置内のいずれかの論理ユニットにアクセスが許可されているパケットのみを通す。このため、基本的にアクセスが許可されていないパケットは、論理ユニットには到達しない。

【００１５】

しかしながら、上述したように、特許文献１のフィルタリング機能は、あくまでも記憶装置アクセス用のパケットのみが存在するネットワークを前提に考えられたものであり、ＩＰネットワークのように想定外のパケットが送信されてくるといった環境を意識した作りではない。

【００１６】

また、特許文献１に開示されている技術では、アクセスが許可されていないと判断されたパケット（以後、不正なパケットと呼ぶ）は処理されずに廃棄されるだけである。

【００１７】

例えば、不正なパケットとしては、その記憶装置にはアクセスが許可されていないホスト計算機からのパケット、そもそも記憶装置自体にアクセスが許可されていない未知の装置からの想定外のパケット、などが考えられる。しかしながら、特許文献１に開示されている技術では、これらの不正なパケットの種別も発信元も判別できない。

【００１８】

ＩＰネットワークなどの記憶装置へのアクセス用のパケット以外も送受信されるような通信回線に接続されている環境では、特に、上記の未知の装置からのパケットに、通信攻撃を意図した悪意を持ったパケットが含まれている可能性が高いが、特許文献１に開示されている技術では、このような通信攻撃に対する積極的な防御対策は考慮されていない。

【００１９】

本発明は、このような状況に鑑みてなされたもので、通信回線に接続された記憶装置において、セキュリティを高めるとともに、記憶装置への通信帯域を確保することを目的とする。

【課題を解決するための手段】

【００２０】

上記目的を達成するために、本発明の記憶装置は、ネットワークからセッション確立時に受信したパケットのうち、正当なパケットのみを記憶装置の論理ユニットに通過させるフィルタリング手段を備える。その際、廃棄するパケットのヘッダ情報等を管理サーバに通知する。通知を受けた管理サーバは、当該ヘッダ情報等を利用して、ネットワーク上の通信を制御する。

【００２１】

例えば、本発明は、ホスト計算機と通信回線を介して接続される記憶装置であって、前記通信回線に接続するためのインタフェースを備え、前記インタフェースは、前記通信回線から通信パケットを受信した際、当該通信パケットの中から前記記憶装置へのアクセス用として予め定められたフォーマットの通信パケットであるか否かを判別する第一のフィルタ手段を備えること
を特徴とする記憶装置を提供する。

【００２２】

また、前記記憶装置は、当該インタフェースにおいて受信した全ての通信パケットの通信量と、前記第一のフィルタ手段において前記フォーマットの通信パケットでないものと判定された通信パケットの通信量とをそれぞれ測定し、両通信量を用いて、通信障害が発生しているか否かを判定する通信障害判定手段と、前記通信障害判定手段において、通信障害が発生していると判断された場合、当該記憶装置に接続され、通知を受けた情報を表示する機能を備える管理サーバに通知する通信障害通知手段とをさらに備え、前記管理サーバは、前記通信障害通知手段から通信障害が発生していると通知を受けた場合、前記通信ログを参照し、通信障害を発生させている前記通信パケットの発信元を抽出する発信元抽出手段と、前記発信元抽出手段で抽出された発信元の情報を元に、当該発信元からの通信を遮断するよう前記通信回線上に備えられた前記記憶装置への通信を中継する中継装置を制御する中継装置制御手段とを備える。

【発明の効果】

【００２３】

本発明によれば、通信回線に接続された記憶装置において、セキュリティを高めることができる。さらに、記憶装置への通信帯域を確保できる。

【発明を実施するための最良の形態】

【００２４】

以下、本発明の一実施形態を、図面を用いて説明する。

【００２５】

ここで、本実施形態では、1以上のホスト計算機と１以上の記憶装置とを備えるストレージシステムにおいて、記憶装置とホスト計算機との間の通信にｉＳＣＳＩを用いる場合を例にあげて説明する。すなわち、本実施形態では、両者間で使用するプロトコルとして、ネットワーク層のプロトコルはＩＰ（Internet Protocol）であり、トランスポート層のプロトコルはＴＣＰ（Transmission Control Protocol）であるＴＣＰ／ＩＰを用い、記憶装置の制御を実施するコマンドセットとして、ＳＣＳＩコマンドを用いる。ＳＣＳＩコマンドは、ＴＣＰ／ＩＰ上をやりとりするパケット内にカプセル化されて送受信される。

【００２６】

もちろん、本発明は、前述のプロトコルやコマンドセットに限定されるものでなく、ホスト計算機から記憶装置にアクセスするためのコマンドセットを、ネットワークで用いられているプロトコル上に実装している仕様であれば、その形式は問わない。

【００２７】

本実施形態の前提である、ｉＳＣＳＩの構成と送受信されるパケットの概念図を図１に示す。本図において、１００は記憶装置、２００はホスト計算機、３００は記憶装置１００とホスト計算機２００との間を接続するＩＰネットワークである。また、本実施形態では、ＩＰネットワーク上を送受信されるＩＰパケットの中で、ＩＰパケットのペイロードに格納されているＴＣＰパケットにＳＣＳＩコマンド、ＳＣＳＩレスポンス等を格納した

ものを、ｉＳＣＳＩパケット３１０と呼ぶ。

【００２８】

ｉＳＣＳＩプロトコルでは、ＳＣＳＩコマンド３１１の発行元をｉＳＣＳＩイニシエータと呼び、受け取ったコマンドを処理してＳＣＳＩコマンド３１１に対するレスポンス３１２を返す側をｉＳＣＳＩターゲットと呼ぶ。従って、本図では、ホスト計算機２００がｉＳＣＳＩイニシエータ、記憶装置１００がｉＳＣＳＩターゲットとなる。

【００２９】

ｉＳＣＳＩの階層モデルでは、ｉＳＣＳＩ層は、ＳＣＳＩコマンドをやりとりするＳＣＳＩ層とＴＣＰ／ＩＰ層との間に位置する。ｉＳＣＳＩ層は、ＳＣＳＩ層からＳＣＳＩコマンド等を受け取り、それをカプセル化してＳＣＳＩ　ＰＤＵ（Protocol Data Unit）を作成し、ＴＣＰ／ＩＰ層に受け渡す。また、ＴＣＰ／ＩＰ層から受け取ったｉＳＣＳＩＰＤＵを処理して、ＳＣＳＩコマンド等を取り出し、それをＳＣＳＩ層に受け渡す。

【００３０】

ｉＳＣＳＩパケット３１０のＴＣＰ／ＩＰ層以下の通信データ構成は、一般的なＴＣＰ／ＩＰパケット構成と同様であり、ｉＳＣＳＩパケット３１０は、カプセル化されたＳＣＳＩコマンドを処理するまでは、通常のＴＣＰ／ＩＰパケットとしてＩＰネットワーク３００上を送受信される。

【００３１】

なお、ｉＳＣＳＩパケット３１０のヘッダには、当該パケットにｉＳＣＳＩコマンドがカプセル化されていることを示す情報が含まれる。このため、ｉＳＣＳＩパケットを受け取ったｉＳＣＳＩターゲット側では、ＴＣＰ／ＩＰ層においてｉＳＣＳＩコマンドを取り出す処理を行わなくても、ヘッダ情報を確認することで、当該パケットが、ｉＳＣＳＩパケット３１０であるか否かを判別できる。

【００３２】

また、ｉＳＣＳＩでは、ｉＳＣＳＩ層において、ｉＳＣＳＩイニシエータ２００とｉＳＣＳＩターゲット１００との間に論理的な通信路であるセッションを確立して通信を行なう。セッションはＴＣＰ層の一般的なコネクションの確立の手続と同様に、認証を得て確立される。認証を得るための手続のことを、ｉＳＣＳＩではｉＳＣＳＩログインと呼ぶ。本実施形態では、セッション確立前、すなわち、ｉＳＣＳＩログイン前の全ＩＰパケット各々についてｉＳＣＳＩパケットであるか否かフィルタリングし、ｉＳＣＳＩパケットであれば、セッションを確立する。そして、セッション確立後は、その認証を信頼してパケットのフィルタリングは行わない。

【００３３】

なお、これらのセッション確立やログインの方法は、従来のＦＣネットワークで接続された記憶装置１００とホスト計算機２００との間のものと同様の仕様である(特許文献１参照)。従って、ＳＣＳＩ層から見た場合、下位の階層の種類、すなわち、ＴＣＰ／ＩＰとＦＣとによるネットワークの種類による違いは無い。

【００３４】

また、特許文献１では、ホスト計算機２００を一意に特定するために、ＦＣフレームヘッダのＳ－ＩＤからＷＷＮを特定するデータ変換が行われている。ｉＳＣＳＩでは、セッション確立時にホスト計算機２００を特定するために、ＩＰネットワーク３００で従来から利用されているドメイン概念のｉＳＣＳＩネームを用いる。ｉＳＣＳＩネームは、ｉＳＣＳＩパケットのヘッダ情報に含まれる。

【００３５】

以上により、ｉＳＣＳＩによる記憶装置１００とホスト計算機２００とのネットワーク接続とは、これまでＦＣネットワークで構成されていたものがＩＰネットワーク３００に取って代わっただけで、記憶装置へのアクセス仕様には全く違いがないことがわかる。

【００３６】

次に、本実施形態のストレージシステムについて説明する。図２は、本実施形態のストレージシステムの機能構成図である。

【００３７】
本図に示すように、本実施形態のストレージシステムは、１以上のホスト計算機２００と、１以上の記憶装置１００と、管理サーバ４００と、ＩＰネットワーク３００とを備える。
【００３８】
ＩＰネットワーク３００は、通信プロトコルにＴＣＰ／ＩＰを利用するネットワークで、インターネットに代表されるように現在全世界的に張り巡らされ、様々な情報機器が接続されるネットワーク環境である。記憶装置１００とホスト計算機２００と管理サーバ４００とは、このＩＰネットワーク３００によって接続される。ｉＳＣＳＩパケットも、他のＩＰパケットと同様に、ＩＰネットワーク３００を介してやり取りされる。
【００３９】
ここで、本実施形態においては、ＩＰネットワーク３００は、ルータもしくはスイッチ３２０によりスター型に接続される構成を例にあげて説明を行なう。しかし、ネットワーク構成はこれに限られない。記憶装置１００とホスト計算機２００との間に、ルータもしくはスイッチ３２０が配置されていればよい。
【００４０】
記憶装置１００は、記憶装置１００外から、ＩＰパケットを受信するストレージ用インタフェース１１０と、記憶領域である論理ユニット（ＬＵ）１３０と、Ｉ／Ｏ命令を受けて論理ユニット１３０の制御を実施する記憶領域制御装置１３１と、記憶装置１００を保守管理する保守用端末１５０と、該保守用端末１５０に記憶装置１００側の情報を通信する通信制御部１６１と、Ｉ／Ｏ処理などの高速化を実現するキャッシュメモリ１６２とを備える。
【００４１】
ここで、ストレージ用インタフェース１１０は、ハードウェア構成として、全体の動作を統括制御する制御プロセッサ１１１と、制御プロセッサ１１１が実行するプログラムを記憶する制御メモリ１１２と、制御プロセッサ１１１停止時もデータを格納する不揮発メモリ１１３と、外部ネットワークとのＩ／Ｆであるポート１１４とを備える。
【００４２】
制御プロセッサ１１１は、制御メモリ１１２に格納されたプログラムを実行することにより、ＩＰレベルフィルタ部１１５と、ＬＵレベルフィルタ部１１６と、通信量測定・判定部１１７と、通信情報および障害通知部１１８と、ｉＳＣＳＩ処理エンジン１１９と、の各機能を実現する。
【００４３】
不揮発メモリ１１３には、上記プログラムを実行する際に使用されるＬＵアクセス許可テーブル１２１と、通信障害判定用閾値テーブル１２２とが格納される。
【００４４】
ＩＰレベルフィルタ部１１５は、セッション確立前のＩＰパケットをフィルタリングする。具体的には、セッション確立前にポート１１４において受信した全てのＩＰパケットのヘッダ情報を参照し、ｉＳＣＳＩパケットであることを示す情報が格納されているか否かにより、当該ＩＰパケットがｉＳＣＳＩパケットであるか否かを判別する。
【００４５】
ｉＳＣＳＩパケットと判別された場合、ＬＵレベルフィルタ部１１６に送出し、その他のＩＰパケット（以後、非ｉＳＣＳＩパケットと呼ぶ）は、通信量測定・判定部１１７を介して通信情報および障害通知部１１８に送出する。
【００４６】
ＬＵレベルフィルタ部１１６は、受け取ったｉＳＣＳＩパケットをフィルタリングする。具体的には、受け取ったｉＳＣＳＩパケットが論理ユニット１３０にアクセス可能か否かを、ｉＳＣＳＩログイン時に受け取ったｉＳＣＳＩパケットのｉＳＣＳＩネームに基づいて後述するＬＵアクセス許可テーブル１２１を参照し判断する。なお、その後、当該ログインが有効である間は、当該ｉＳＣＳＩネームを有するｉＳＣＳＩパケットの論理ユニ

ット１３０へのアクセス可否のチェックは行わない。

【００４７】

アクセス可能なｉＳＣＳＩパケット（以後、許可ｉＳＣＳＩパケットと呼ぶ）は、通信量測定・判定部１１７を介してｉＳＣＳＩ処理エンジン１１９に送出する。アクセス許可のないｉＳＣＳＩパケット（以後、不許可ｉＳＣＳＩパケットと呼ぶ）は、通信量測定・判定部１１７を介して通信情報および障害通知部１１８に送出する。

【００４８】

ここで、ＬＵアクセス許可テーブル１２１について説明する。ＬＵアクセス許可テーブル１２１は、ホスト計算機毎に、アクセスが許可されている論理ユニット１３０を対応づけて格納したものである。図３にＬＵアクセス許可テーブル１２１の一例を示す。

【００４９】

本図に示すように、ＬＵアクセス許可テーブル１２１は、ホスト計算器２００を一意に特定するｉＳＣＳＩネーム１２１１と、ユーザやホスト計算機２００上のオペレーティングシステムが論理ユニット１３０に任意に割当てた仮想的な論理ユニット番号(仮想ＬＵＮ)１２１２と、仮想ＬＵＮ１２１２に対応する記憶装置１００上で論理ユニット１３０を一意に特定する論理ユニット番号（ＬＵＮ）１２１３とを備える。このＬＵアクセス許可テーブル１２１は、管理者などにより予め、管理サーバ４００などから設定される。

【００５０】

ＬＵレベルフィルタ部１１６が受け取ったｉＳＣＳＩパケットのヘッダに格納されているｉＳＣＳＩネームと同じｉＳＣＳＩネームが、ＬＵアクセス許可テーブル１２１のｉＳＣＳＩネーム１２１１に格納され、それに対応する仮想ＬＵＮ１２１２、ＬＵＮ１２１３が格納されていれば、アクセスが許可されていることを意味する。なお、ＬＵレベルフィルタ部１１６におけるアクセス可否の判定方法については、特許文献１の方法と同様であるため、ここではその説明を省略する。

【００５１】

通信量測定・判定部１１７は、ＩＰレベルフィルタ部１１５およびＬＵレベルフィルタ部１１６の２つのフィルタ手段で分別された３種のパケット（許可ｉＳＣＳＩパケット、不許可ｉＳＣＳＩパケット、非ｉＳＣＳＩパケット）を受け取り、それぞれの単位時間当たりの通信量を測定した後、受け取ったパケットの種類に応じて、通信情報および障害通知部１１８、または、ｉＳＣＳＩ処理エンジン１１９に送出する。また、単位時間当たりの測定結果を用いて、通信障害判定用閾値テーブル１２２に従って通信障害発生の有無を判定する。

【００５２】

ここで、通信障害判定用閾値テーブル１２２は、判定対象ごとに、その閾値とともに判断基準が格納されているテーブルである。図４に通信障害判定用閾値テーブル１２２の一例を示す。

【００５３】

本実施形態の通信障害判定用閾値テーブル１２２は、判定対象通信比の内容を格納する判定対象通信比格納欄１２２ａと、通信障害と判定する閾値とともに判断基準を格納する閾値格納欄１２２ｂとを備える。

【００５４】

本実施形態では、判定対象通信比として、例えば、非ｉＳＣＳＩパケットの単位時間当たりの通信量がストレージ用インタフェース１１０において受信した全パケットの単位時間当たりの通信量に対して占める割合１２２１（以後、非ｉＳＣＳＩパケット比と呼ぶ。）、不許可ｉＳＣＳＩパケットの単位時間当たりの通信量がＩＰレベルフィルタ部１１５において判別された全てのｉＳＣＳＩパケットの単位時間あたりの通信量に対して占める割合１２２２（以後、不許可ｉＳＣＳＩパケット比と呼ぶ。）、および、許可ｉＳＣＳＩパケットの単位時間あたりの通信量がストレージ用インタフェース１１０において受信した全パケットの単位時間当たりの通信量に占める割合１２２３（以後、許可ｉＳＣＳＩパケット比と呼ぶ。）などが格納される。

【００５５】
なお、それぞれの比から判定される通信障害とは、例えば、非ｉＳＣＳＩパケット比の場合、不正なパケットによる通信攻撃によるもの、不許可ｉＳＣＳＩパケット比の場合、既に記憶装置１００にアクセス権を有していない状態となったホスト計算機２００が、何らかの事情で、そのままアクセスを続けていることによるもの、許可ｉＳＣＳＩパケット比の場合、通信帯域設定が適切でないことによるものである。閾値格納欄１２２ｂには、これらの通信障害の発生が判定できる値および基準が格納される。
【００５６】
本実施形態では、通信量測定・判定部１１７は、それぞれの測定結果から得られる通信比の値が、閾値格納欄１２２ｂに格納されている条件を満たす場合、通信障害と判定し、通信障害が発生した旨、通信障害が発生したと判断した通信比の種類（障害種別：非ｉＳＣＳＩパケット比、不許可ｉＳＣＳＩパケット比、または、許可ｉＳＣＳＩパケット比など）、通信障害が発生したと判断した際の通信比の値、通信障害が発生したと判断した通信量を測定した単位時間の時間情報（障害時刻）、および、通信障害が発生したと判断した際のパケットの通信情報を、通信情報および障害通知部１１８に通知する。ここで、通知する通信情報は、後述の通信ログ１５８において説明する。
【００５７】
例えば、全パケットの通信量が１５０ＫＢｙｔｅ／ｓの時、非ｉＳＣＳＩパケットの通信量が１００ＫＢｙｔｅ／ｓあったとすると、通信障害判定用閾値テーブル１２２の非ｉＳＣＳＩパケット比１２２１の値は６６％となり、閾値格納部１２２ｂに格納されている「５０％以上」に該当する。このような場合、通信量測定・判定部１１７は、ｉＳＣＳＩパケットの正常な通信に問題が出る程度の通信が記憶装置１００に届いている、すなわち、障害発生と判定する。
【００５８】
なお、本図に示す判定対象通信比は一例であり、ＩＰレベルフィルタ部１１５およびＬＵレベルフィルタ部１１６の２つのフィルタ手段で判別される３つのパケットに関する情報から測定される任意の通信量を用いて得られる各種の通信比を判定対象として用いることが可能である。
【００５９】
通信情報および障害通知部１１８は、ＩＰレベルフィルタ部１１５およびＬＵレベルフィルタ部１１６の２つのフィルタ部から、通信量測定・判定部１１７を介して受け取ったパケット、および、通信量測定・判定部１１７において通信障害と判定された場合に受け取った情報を保守用端末１５０に送信する。
【００６０】
ｉＳＣＳＩ処理エンジン１１９は、ＩＰレベルフィルタ部１１５およびＬＵレベルフィルタ部１１６を経て受け取った許可ｉＳＣＳＩパケットに対し、ｉＳＣＳＩターゲットとしての処理を施し、ＳＣＳＩコマンドを取り出し、送信先として指定された論理ユニット１３０に送信する。
【００６１】
なお、上記機能を実現するプログラムは、制御メモリ１１２ではなく、制御プロセッサ１１１が読み取り可能な記録媒体（フレキシブルディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、半導体メモリ、ＬＡＮ及びＳＡＮ等の伝送経路等）に格納されていても良い。また、これらのプログラムは、その機能をハードウェア構成（ＬＳＩ（Large Scale Integration）等の半導体集積回路等）で実現しても良い。
【００６２】
保守用端末１５０は、ハードウェア構成として、保守用端末１５０全体の動作を統括制御する制御プロセッサ１５１と、制御プロセッサ１５１が実行するプログラムを記憶する制御メモリ１５２と、データを記録保存する保守用端末記憶領域１５３と、外部ネットワークとのインタフェース１５４と、記憶装置１００本体とのインタフェース１５５とを備える。

【００６３】
制御プロセッサ１５１は、制御メモリ１５２に格納されたプログラムを実行することにより、通信情報記録部１５６と、警告メッセージ通報部１５７と、の各機能を実現する。
【００６４】
保守用端末記憶領域１５３には、通信ログ１５８が記録保存される。
【００６５】
通信情報記録部１５６は、通信情報および障害通知部１１８から送付されてきたパケットの通信情報を通信ログ１５８として保守用端末記憶領域１５３に記録する。
【００６６】
ここで、通信ログ１５８に記録される情報を説明する。図５に本実施形態における通信ログ１５８の一例を示す。
【００６７】
記録されるパケットの通信情報は、例えば、本図に示すように、当該通信情報が記録された日時１５８１、当該通信のパケットのプロトコルの種類１５８２、送信元のＩＰアドレスおよび使用ポート番号１５８３、送信先のＩＰアドレスおよび使用ポート番号１５８４、などである。
【００６８】
なお、ここで示す通信ログは一例であり、以上の情報が最低限含まれていれば、その記録形式、および、その他の情報の有無は問わない。
【００６９】
警告メッセージ通報部１５７は、通信情報および障害通知部１１８から送付されてきた通信障害が発生した旨の通知、障害種別、通信比の値、および、障害時刻の情報を用い、予め障害種別毎に用意されているテキストメッセージと組み合わせて警告メッセージを生成し、管理サーバ４００に通報する。
【００７０】
なお、これらの機能を実現するプログラムは、制御プロセッサ１５１により読み取り可能な記録媒体（フレキシブルディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、半導体メモリ、ＬＡＮ及びＳＡＮ等の伝送経路等）に格納しても良い。
【００７１】
また、これらプログラムは、その機能をハードウェア構成（ＬＳＩ（Large Scale Integration）等の半導体集積回路等）で実現しても良い。
【００７２】
なお、本実施形態では、保守用端末１５０を記憶装置１００内に含む構成を例にあげて説明するが、保守用端末１５０の構成はこれに限られない。例えば、記憶装置１００外に備えられる構成であってもよい。また、複数の記憶装置１００について、１つの保守用端末１５０を備えるよう構成してもよい。
【００７３】
ホスト計算機２００は、ハードウェア構成として、全体の動作を統括制御する制御プロセッサ２０１と、制御プロセッサ２０１が実行するプログラムを記憶する制御メモリ２０２と、外部ネットワークとのインタフェース２０３とを備える。
【００７４】
ホスト計算機２００は、制御メモリ２０２上に、ＳＣＳＩコマンドを伝送フレームに格納することにより、ｉＳＣＳＩパケットを生成するｉＳＣＳＩドライバ２１１を備える。
【００７５】
なお、ｉＳＣＳＩドライバ２１１は、制御プロセッサ２０１により実行されることによりその機能が実現されるプログラムである。また、このプログラムは、制御プロセッサ２０１により読み取り可能な記録媒体（フレキシブルディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、半導体メモリ、ＬＡＮ及びＳＡＮ等の伝送経路等）に格納しても良い。また、これらプログラムは、その機能をハードウェア構成（ＬＳＩ（Large Scale Integration）等の半導体集積回路等）で実現しても良い。

【００７６】
管理サーバ４００は、ハードウェア構成として、全体の動作を統括制御する制御プロセッサ４０１と、制御プロセッサ４０１が実行するプログラムを記憶する制御メモリ４０２と、外部ネットワークとのインタフェース４０３と、入出力装置とのＩ／Ｆ４０４と、入力装置４０５と、出力装置４０６とを備える。
【００７７】
制御プロセッサ４０１は、制御メモリ４０２に格納されたプログラムを実行することにより、帯域条件指定部４１１と、障害情報表示部４１２と、不正通信発生元解析部４１３と、ルータ・スイッチ制御指示部４１４との各機能を実現する。
【００７８】
障害情報表示部４１２は、管理サーバ４００に記憶装置１００から警告メッセージが送付されてきた際に、送付されてきた警告メッセージが示す情報を出力装置４０６に表示する。
【００７９】
帯域条件指定部４１１は、記憶装置１００から警告メッセージが送付されてきた際にＩＰネットワーク上で確保したい通信帯域の情報を、管理者から入力装置４０５を介して受け付け、設定する。設定時期は、システムの構築が完了した後、必要に応じて管理者が決定する。例えば、構築直後、あるいは、出力装置４０６に表示された警告メッセージの内容を見た管理者が再設定が必要と判断した場合などである。
【００８０】
さらに、警告メッセージを受け取った際、当該障害種別が、許可ｉＳＣＳＩパケット比１２２３を示すものであった場合、帯域条件指定部４１１は、通信障害判定用閾値テーブル１２２にアクセスし、警告メッセージ内の通信比の値と、通信障害判定閾値テーブル１２２の対応する通信比の閾値格納欄１２２ｂに設定されている最新の閾値および判断基準とを比較し、通信帯域を再調整する必要があるか否かを判断する。
【００８１】
具体的な判定例を以下に挙げる。例えば、管理者により、ルータ・スイッチ３２０が、記憶装置１００の論理ユニット１３０へのアクセスに使用する帯域において、誤差１０％未満で、全体通信量の７０％をｉＳＣＳＩパケット用に確保するよう制御するように設定されているとする。この場合、通信障害判定用閾値テーブル１２２には、図４に示すように、正常な制御範囲を超えたか否かを判定する閾値および判断基準として６０％以下が設定される。このような設定がなされている時に、許可ｉＳＣＳＩパケット比が６０％以下に落ち込んだ場合、すなわち、ルータ・スイッチ３２０によって、帯域制御が設定どおりになされていない状態になった場合、通信量測定・判定部１１７によって、障害発生と判定されることにより、その状態が検出され、警告メッセージ通報部１５７を介して、管理サーバ４００に通知がなされる。
【００８２】
通常は、通信障害判定用閾値テーブル１２２の閾値格納欄１２２ｂに格納されている判断基準に合致した場合、警告メッセージが発行されるため、警告メッセージが発行されれば、再調整が必要となる。しかし、通信障害判定用閾値テーブル１２２の閾値および判断基準は、警告メッセージ発生時の値等から変更されていることがありえる。このため、帯域条件指定部４１１において、一旦判断を行う。
【００８３】
そして、判断結果が再調整が必要であるもの、すなわち、通信障害判定用閾値テーブル１２２に設定されている判断基準に合致するものであった場合は、後述するルータ・スイッチ制御指示部４１４に向けて、帯域を調整するための制御命令を発行する。
【００８４】
ここで、制御命令は、例えば、許可ｉＳＣＳＩパケットのスループットが、ターゲットとしている帯域に近づくよう、ルータ・スイッチの構成を変更するもので、例えば、ルータ・スイッチにおけるキューイング待ち時間等を長くするといったパラメータ値を変更す

るものがある。

【００８５】

不正通信発生元解析部４１３は、管理サーバ４００に記憶装置１００から警告メッセージが送付されてきた際に、警告メッセージ内の障害時刻の情報を元に、保守用端末の記憶領域１５３に記録されている通信ログ１５８にアクセスし、大量に非ｉＳＣＳＩパケットを送信してくるといった通信攻撃と考えられる不正通信の発行元を解析する。

【００８６】

具体的な解析例を以下に説明する。例えば、前述の通信量測定・判定部１１７が、図５に示す通信ログ１５８群を基に、単位時間として２００３年７月１５日１０：００：０１から１０：００：０２の１秒間の通信量を測定し、閾値を越えているため、障害発生と判断したものとする。ここで、図５に示す通信ログの場合、２００３年７月１５日１０：００：０１から１０：００：０２の間に、非ｉＳＣＳＩパケットが、同じ発信元から多量に届いている。

【００８７】

この場合、警告メッセージには、障害時刻として２００３年７月１５日１０：００：０１が格納される。不正通信発生元解析部４１３は、この警告メッセージ内の障害時刻に該当する通信ログ１５８を抽出する。

【００８８】

その中から非ｉＳＣＳＩパケットを抽出し、送信元毎に、通信量を得る。そして、所定の通信量を超えるなどした送信元のアドレス情報１５８３を抽出する。

【００８９】

そして、後述するルータ・スイッチ制御指示部４１４に向けて、当該不正通信の発行元からの通信を遮断することを指示する制御命令を発行する。

【００９０】

ルータ・スイッチ制御指示部４１４は、管理サーバ４００に記憶装置１００から警告メッセージが送付されてきた際に、帯域条件指定部４１１および不正通信発生元解析部４１３から発行された制御命令に従って、ルータ・スイッチ３００を制御し、不正通信の発行元からのパケットを遮断し、正常アクセスのパケットの帯域を確保する。

【００９１】

なお、これらの機能を実現するプログラムは、制御プロセッサ４０１により読み取り可能な記録媒体（フレキシブルディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、半導体メモリ、ＬＡＮ及びＳＡＮ等の伝送経路等）に格納されても良い。

【００９２】

また、これらプログラムは、その機能をハードウェア構成（ＬＳＩ（Large Scale Integration）等の半導体集積回路等）で実現しても良い。

【００９３】

次に、上記の機能を有する本実施形態のストレージシステムにおいて、記憶装置１００がパケットを受信した場合の処理流れの概要を説明する。図６は、本実施形態のシステムを構成する要素のうち、処理の概要を説明するために代表的なものを記載した構成図である。

【００９４】

ここで、本図において、矢印００１～００３の向きに送信されるパケットを、それぞれ、パケット００１、パケット００２、パケット００３と呼ぶ。これらは、ｉＳＣＳＩターゲットである記憶装置１００に、ＩＰネットワーク３００から送信されるパケットである。この中で、パケット００１は、許可ｉＳＣＳＩパケット、パケット００２は、不許可ｉＳＣＳＩパケット、パケット００３は発信元が不明な情報機器から、記憶装置１００に向け発信された非ｉＳＣＳＩパケットとする。

【００９５】

記憶装置１００上のストレージ用インタフェース１１０は、パケット００１、００２、００３を受信すると、ＩＰレベルフィルタ部１１５により、受信したパケットを選別する

。ここでは、パケット００１およびパケット００２がｉＳＣＳＩパケットと判断され、ＬＵレベルフィルタ部１１６に向けて送出される。一方、パケット００３は、破棄するものとして矢印００４に従って、通信量測定・判定部１１７を介して通信情報および障害通知部１１８に向けて送出される。通信量測定・判定部１１７では、パケット００３の単位時間当たりの通信量を測定し、必要な通信比を算出し、通信障害判定用閾値テーブル１２２を参照しながら、通信障害の発生をモニタする。

【００９６】

一方、ＩＰレベルフィルタ部１１５からＬＵレベルフィルタ部１１６に向けて送出されたｉＳＣＳＩパケットであるパケット００１および００２は、ＬＵレベルフィルタ部１１６により、ＬＵアクセス許可テーブル１２１を参照しながら、記憶装置１００内論理ユニット１３０にアクセスが許可されているパケットであるか判断される。

【００９７】

そして、ＬＵレベルフィルタ部１１６は、パケット００２を廃棄するものとして、矢印００５に従って、通信量測定・判定部１１７を介して通信情報および障害通知部１１８に向けて送出する。通信量測定・判定部１１７では、パケット００２の単位時間当たりの通信量を測定し、必要な通信比を算出し、通信障害判定用閾値テーブル１２２を参照しながら、通信障害の発生をモニタする。

【００９８】

一方、ＬＵレベルフィルタ部１１６は、パケット００１を、論理ユニット１３０にアクセスが許可されているパケットであると判断し、矢印００６に従って通信量測定・判定部１１７を介してｉＳＣＳＩエンジン１１９に向けて送出する。ｉＳＣＳＩ処理エンジン１１９においてＳＣＳＩコマンドが取り出され、取り出されたｉＳＣＳＩコマンドが論理ユニット１３０に送られ、Ｉ／Ｏ処理が実施される。

【００９９】

なお、通信量測定・判定部１１７では、パケット００１'の単位時間当たりの通信量を測定し、必要な通信比を算出し、通信障害判定用閾値テーブル１２２を参照しながら、通信障害の発生をモニタする。

【０１００】

通信情報および障害通知部１１８は、図６の矢印００７に従って、パケット００２および００３の通信情報を記憶装置１００内の保守用端末１５０の通信情報記録部１５６に送信する。その後、通信情報記録部１５６は、パケット００２および００３の通信情報を、通信ログ１５８として記録する。

【０１０１】

また、通信量測定・判定部１１７は、通信障害判定用閾値テーブル１２２の閾値を利用して、通信障害が発生しているか否か判定する。

【０１０２】

判定で通信障害が発生していると判断された場合には、図６の矢印００８に従って、通信情報および障害通知部１１８を介して、保守用端末１５０内の警告メッセージ通報部１５７に情報が伝達され、図６の矢印００９に従って、それを受けた警告メッセージ通報部１５７が警告メッセージを発信することにより、管理サーバ４００にその旨を通報する。

【０１０３】

警告メッセージを受けた管理サーバ４００は、それぞれの通信障害に応じた警告メッセージを表示することにより管理者に情報を提示する。また、警告メッセージに応じた適切な性能低下防止処理を実行する。

【０１０４】

以下に、警告メッセージが管理サーバ４００に送信される処理の流れ、および、警告メッセージを受けた場合に管理サーバ４００が行う性能低下防止処理について説明する。

【０１０５】

図７は、不適切なパケット（不許可ｉＳＣＳＩパケット、非ｉＳＣＳＩパケット）を受信した場合の、本実施形態のストレージシステム内の処理フローを示す。

【０１０６】
まず、通信量測定・判定部１１７は、ＩＰレベルフィルタ部１１５および/またはＬＵレベルフィルタ部１１６を経て廃棄（論理ユニット１３０に送信しない）と判定されたパケット、および、ストレージ用インタフェース１１０で受信した全パケットについて、単位時間当たり(例えば、１秒)の通信量を測定し、測定した単位時間毎に、予め定めた通信比を算出する（ステップ０１００）。
【０１０７】
次に通信量測定・判定部１１７は、算出された通信比を基に、通信障害判定用閾値テーブル１２２を参照し、障害と判定する基準に該当するか否か判定する(ステップ０１１０)。
【０１０８】
ステップ０１１０で通信障害判定用閾値テーブル１２２に該当する項目が無い場合(Ｎｏの場合)は、ステップ０１００に戻り、再度処理を開始する。
【０１０９】
一方、ステップ０１１０で通信障害判定用閾値テーブル１２２に該当する項目がある場合(Ｙｅｓの場合)は、通信量測定・判定部１１７は、障害種別（不許可パケット比、または、非ｉＳＣＳＩパケット比）等を、障害通知部１１８を介して、警告メッセージ通報部１５７に通知する(ステップ０１２０)。
【０１１０】
通知を受けた警告メッセージ通報部１５７は、障害種別に応じた警告メッセージを生成し、障害情報として管理サーバ４００に通報する(ステップ０１３０)。
【０１１１】
警告メッセージを受けた管理サーバ４００は、障害情報表示部４１１に、出力装置４０６に前記障害メッセージの内容を表示させ、管理者に提示する（ステップ０１４０）。管理者は、表示内容を確認することにより、現在の記憶装置１００の通信状態を把握することができ、例えば、帯域の再設定などの処理を行うことができる。
【０１１２】
管理サーバ４００は、上記のように、警告メッセージを受け取った際、その内容を出力装置４０６に提示することにより、管理者の注意を促し、管理者の対処を受け付けるだけでなく、自ら、受け取った警告メッセージの内容に応じて、ストレージシステムの性能低下防止処理を行うことができる。
【０１１３】
次に上記のステップ０１３０において、受け取った警告メッセージが、非ｉＳＣＳＩパケット比が、閾値が超えることを意味するものであった場合、または、不許可ｉＳＣＳＩパケット比が、閾値を越えることを意味するものであった場合、すなわち、不適切なパケットのアクセスが増えた場合、管理サーバ４００が行う性能低下防止処理について説明する。ここで、管理サーバ４００が行う性能低下防止処理とは、記憶装置のＩ／Ｏ性能低下をもたらしているパケットを遮断することである。
【０１１４】
なお、本実施形態では、非ｉＳＣＳＩパケット比が閾値を越えた場合を例に、管理サーバ４００において、通信ログ１５８の内容を解析して不正通信の発行元を突き止め、記憶装置１００への通信路のＩＰネットワーク３００上にあるルータ、スイッチ３２０などのＩＰネットワーク中継器機を制御し、当該不正通信の発行元からの通信を遮断するといった処理を説明する。
【０１１５】
図８に、不正なアクセスが増えた場合、管理サーバ４００においてなされる処理のフローを示す。
【０１１６】
まず、管理サーバ４００は、保守用端末１５０から、障害種別が非ｉＳＣＳＩパケット比が閾値を超えたことを示す警告メッセージを受け取る(ステップ０２００)。

【０１１７】
警告メッセージを受けた管理サーバ４００は、障害情報表示部４１２にステップ０２００で受け取った警告メッセージに応じた表示を出力装置４０６に表示させるとともに、不正通信発生元解析部４１３に保守用端末１５０に記録されている通信ログ１５８を取得させる(ステップ０２１０)。
【０１１８】
不正通信発生元解析部４１３は取得した通信ログ１５８の情報を用いて、該当する通信ログを解析し、不正なパケットの送信元のアドレス情報等を抽出する(ステップ０２２０)。
【０１１９】
不正通信発生元解析部４１３は、該当アドレス１５８３(例えば、図５の例の場合１０．Ｘ．Ｘ．Ｘ)からのパケットを全て遮断する処置を実行するため、ルータ・スイッチ制御指示部４１４に、当該アドレス１５８３からの通信を遮断することを意味するルータもしくはスイッチの制御命令を発行する(ステップ０２３０)。
【０１２０】
ルータ・スイッチ制御指示部４１４は、ステップ０２３０で発行された制御命令に従い、該当アドレスからのパケットを遮断するようルータもしくはスイッチ３２０を制御する(ステップ０２４０)。
【０１２１】
本実施形態のストレージシステムは、上記のような処理を行うことにより、記憶装置１００を攻撃対象とした通信攻撃を遮断することができる。
【０１２２】
次に、上記のステップ１３０において、受け取った警告メッセージが、正常に論理ユニット１３０にアクセスするｉＳＣＳＩパケットの通信量の割合が減ったことを意味するものであった場合、すなわち、許可ｉＳＣＳＩパケット比が閾値以下となった場合の処理について、以下に説明する。
【０１２３】
ここで、管理サーバ４００が行う性能低下防止処理とは、予め管理者により指定されたＩＰネットワークの帯域制御に関する指示に基づき、許可ｉＳＣＳＩパケットに、必要な帯域を確保することである。管理サーバ４００が、記憶装置１００への通信路のＩＰネットワーク３００上にあるルータ、スイッチ３２０などのＩＰネットワーク中継器機を制御し、記憶装置１００にアクセス権限のあるホスト計算機２００からのアクセスのために必要な帯域を確保する。
【０１２４】
図９に、許可ｉＳＣＳＩパケット比が閾値以下となった場合、管理サーバ４００においてなされる処理のフローを示す。
【０１２５】
まず、管理サーバ４００は、保守用端末１５０から、許可ｉＳＣＳＩパケット比が閾値以下となったことを示す警告メッセージを受け取る(ステップ０３００)。
【０１２６】
警告メッセージを受け取った管理サーバ４００は、障害情報表示部４１２に受け取った警告メッセージの内容に応じた表示を表示装置４０６に表示させるとともに、帯域制御条件指定部４１１に警告メッセージに含まれる情報を通知する(ステップ０３１０)。
【０１２７】
帯域制御条件指定部４１１は、通信障害判定用閾値テーブル１２２の閾値格納欄１２２ｂに格納されている値と、警告メッセージによって受け取った通信量比の値とを比較し、帯域制御の設定が妥当なものかどうか、つまり再調整が必要かを判定する(ステップ０３２０)。
【０１２８】
ステップ０３２０における判定で帯域制御の再調整が必要と判断された場合(Ｙｅｓの

場合)、ルータ・スイッチ制御指示部４１４に、与えられた帯域制御を実施するために必要な命令を送付する（０３３０）。

【０１２９】

一方、再調整が必要ないと判断された場合(Ｎｏの場合)、処理を終了する。

【０１３０】

ステップ０３３０で命令を受けたルータ・スイッチ制御指示部４１４は、ルータのコマンド等で指定された条件の帯域制御設定を再調整し（０３４０）、処理を終了する。

【０１３１】

本実施形態のストレージシステムは、上記のような処理を行うことにより、通信状態に応じて、記憶装置１００に対する帯域設定を動的に再調整することが可能となる。

【０１３２】

このように、本実施形態によれば、ストレージシステムは、記憶装置１００において、論理ユニット１３０にアクセス可能なパケット（正常なパケット）とそれ以外のパケット（不正なパケット）とを振り分けることができる。

【０１３３】

本実施形態では、この振り分けを、受け取ったパケットから、ｉＳＣＳＩパケットのみを抽出するＩＰレベルフィルタ（第一のフィルタ）と、ｉＳＣＳＩパケットから記憶装置にアクセスが許可されているパケットのみを抽出するＬＵレベルフィルタ（第二のフィルタ）との２つのフィルタにより実現している。しかも、ＬＵレベルフィルタでのアクセス可否の判断は、セッションの確立時、すなわち、ｉＳＣＳＩログイン時に送信されるｉＳＣＳＩパケットのみで行われる。そして、当該パケットによりセッションが確立した後は、個々のパケットのアクセスの可否を判断しない。このため、効率よくアクセスの可否を判断できる。

【０１３４】

また、不正なパケットと振り分けられたものの通信ログを記録しているため、当該情報を用いて、今後の受信を遮断する措置をとることができる。

【０１３５】

さらに、全パケットについて、振り分けられた種別毎に通信量をモニタしているため、当該情報を用いて、正常なパケットの通信のための適切な帯域を確保することもできる。

【図面の簡単な説明】

【０１３６】

【図１】図１は、本実施形態のｉＳＣＳＩパケットを説明するための図である。

【図２】図２は、本実施形態のストレージシステムの機能構成図である。

【図３】図３は、本実施形態のＬＵアクセス許可テーブルを説明するための図である。

【図４】図４は、本実施形態の通信障害判定用閾値テーブルを説明するための図である。

【図５】図５は、本実施形態の通信ログを説明するための図である。

【図６】図６は、本実施形態において、記憶装置がパケットを受信した際の処理の流れを説明するための図である。

【図７】図７は、本実施形態のストレージシステムにおいて、不適切なパケットを受信した場合の処理フローである。

【図８】図８は、本実施形態の管理サーバにおける性能低下防止処理の処理フローである。

【図９】図９は、本実施形態の管理サーバにおける帯域制御処理の処理フローである。

【符号の説明】

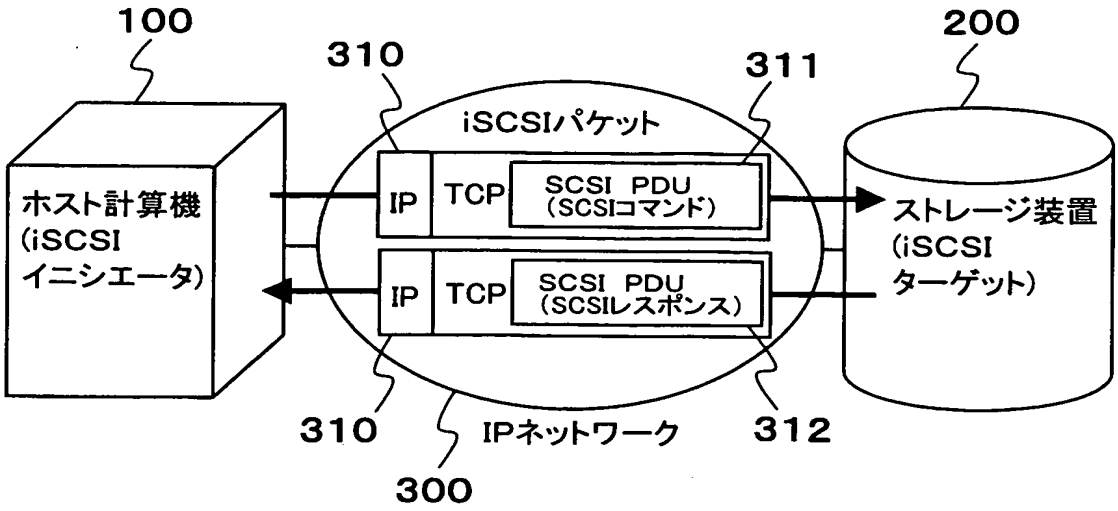
【０１３７】

１００…記憶装置、１１０…ストレージ用インタフェース、１１１…制御プロセッサ、１１２…制御メモリ、１１３…不揮発メモリ、１１４…ポート、１１５…ＩＰレベルフィル

タ部、１１６…ＬＵレベルフィルタ部、１１７…通信量測定・判定部、１１８…通信情報および障害通知部、１１９…ｉＳＣＳＩ処理エンジン、１２１…ＬＵアクセス許可テーブル、１２２…通信障害判定用閾値テーブル、１３０…論理ユニット、１３１…記憶領域制御装置、１５０…保守用端末、１５１…制御プロセッサ、１５２…制御メモリ、１５３…保守用端末記憶領域、１５４…インタフェース、１５５…インタフェース、１５６…通信情報記録部、１５７…警告メッセージ通報部、１５８…通信ログ、１６１…通信制御部、１６２…キャッシュメモリ、２００…ホスト計算器、２０１…制御プロセッサ、２０２…制御メモリ、２０３…Ｉ／Ｆ、２１１…ｉＳＣＳＩドライバ、３００…ＩＰネットワーク、３１０…ｉＳＣＳＩパケット、３１１…ＳＣＳＩコマンド、３１２…ＳＣＳＩレスポンス、３２０…ルータまたはスイッチ、４００…管理サーバ、４０１…制御プロセッサ、４０２…制御メモリ、４０３…Ｉ／Ｆ、４０４…Ｉ／Ｆ、４０５…入力装置、４０６…出力装置、４１１…帯域条件指定部、４１２…障害情報表示部、４１３…不正通信元解析部、４１４…ルータ・スイッチ制御指示部、

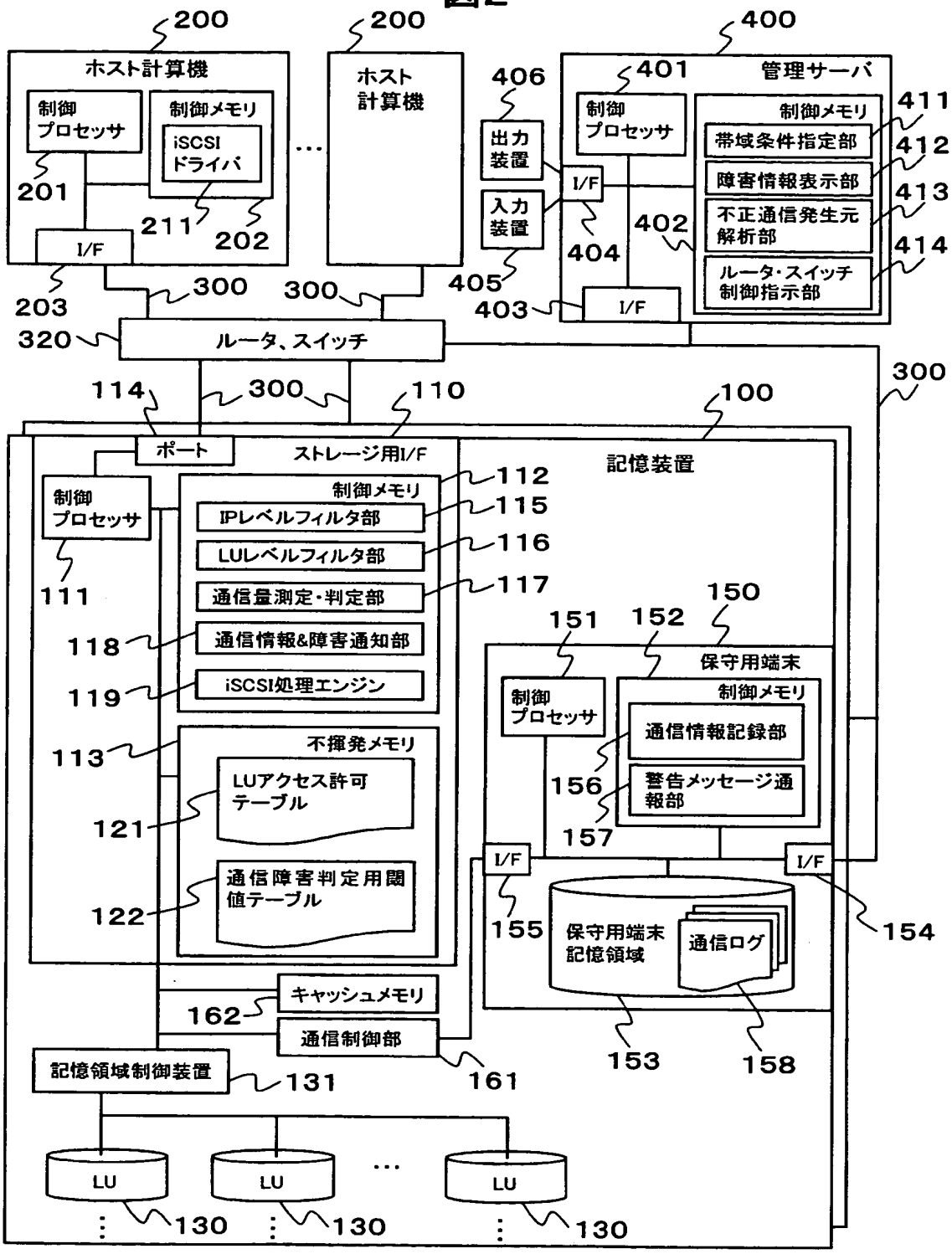
【書類名】図面
【図１】

図1


100
310
311
200
iSCSIパケット
ホスト計算機
(iSCSI
イニシエータ)
IP
TCP
SCSI PDU
(SCSIコマンド)
IP
TCP
SCSI PDU
(SCSIレスポンス)
ストレージ装置
(iSCSI
ターゲット)
310
IPネットワーク
312
300

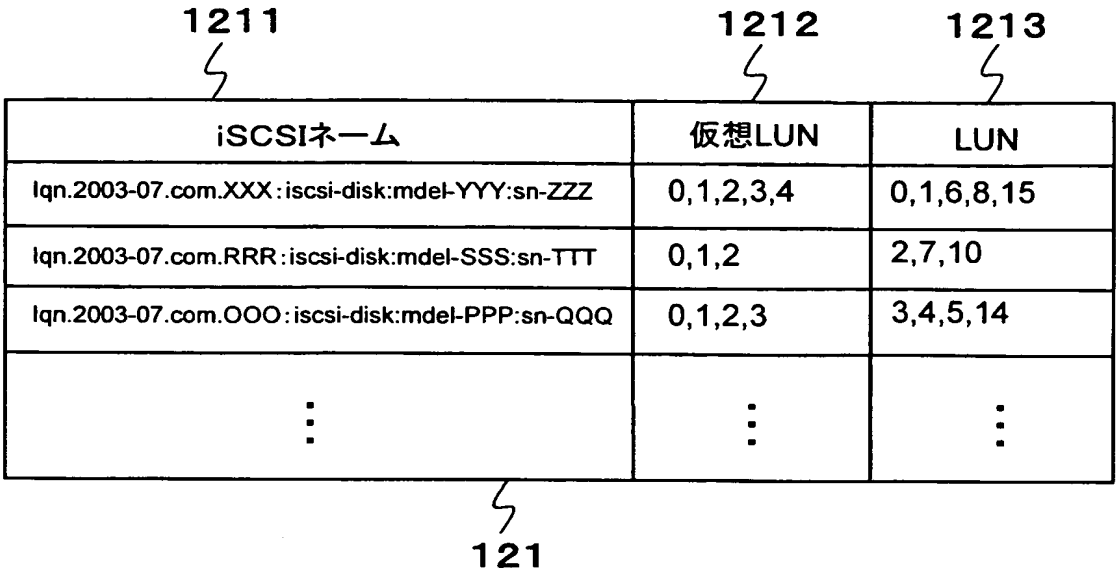
【図２】

図2


200
200
400
ホスト計算機
制御プロセッサ
制御メモリ
iSCSIドライバ
201
211
202
I/F
203
ホスト計算機
406
出力装置
入力装置
405
401
管理サーバ
制御プロセッサ
I/F
404
403
I/F
制御メモリ
411
帯域条件指定部
412
障害情報表示部
413
不正通信発生元解析部
402
414
ルータ・スイッチ制御指示部
300
300
320
ルータ、スイッチ
300
114
300
110
100
ポート
ストレージ用I/F
記憶装置
制御プロセッサ
111
制御メモリ
112
IPレベルフィルタ部
115
LUレベルフィルタ部
116
通信量測定・判定部
117
118
通信情報&障害通知部
119
iSCSI処理エンジン
113
不揮発メモリ
LUアクセス許可テーブル
121
通信障害判定用閾値テーブル
122
150
151
152
保守用端末
制御プロセッサ
制御メモリ
通信情報記録部
156
警告メッセージ通報部
157
I/F
I/F
155
154
保守用端末記憶領域
通信ログ
153
158
キャッシュメモリ
162
通信制御部
161
記憶領域制御装置
131
LU
LU
LU
130
130
130

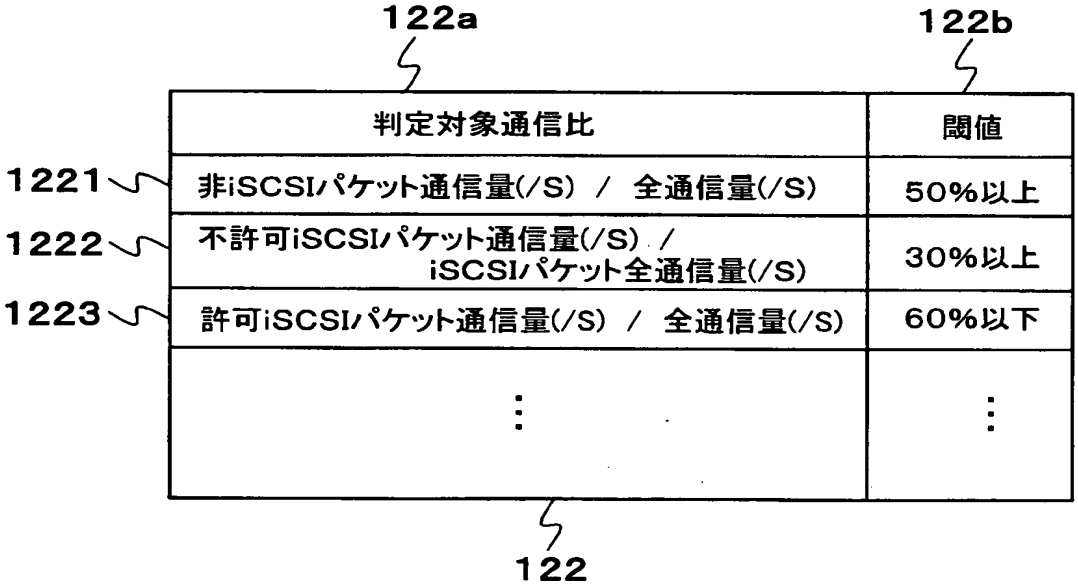
【図３】

図3


1211
1212
1213
iSCSIネーム
仮想LUN
LUN
Iqn.2003-07.com.XXX:iscsi-disk:mdel-YYY:sn-ZZZ
0,1,2,3,4
0,1,6,8,15
Iqn.2003-07.com.RRR:iscsi-disk:mdel-SSS:sn-TTT
0,1,2
2,7,10
Iqn.2003-07.com.OOO:iscsi-disk:mdel-PPP:sn-QQQ
0,1,2,3
3,4,5,14
121

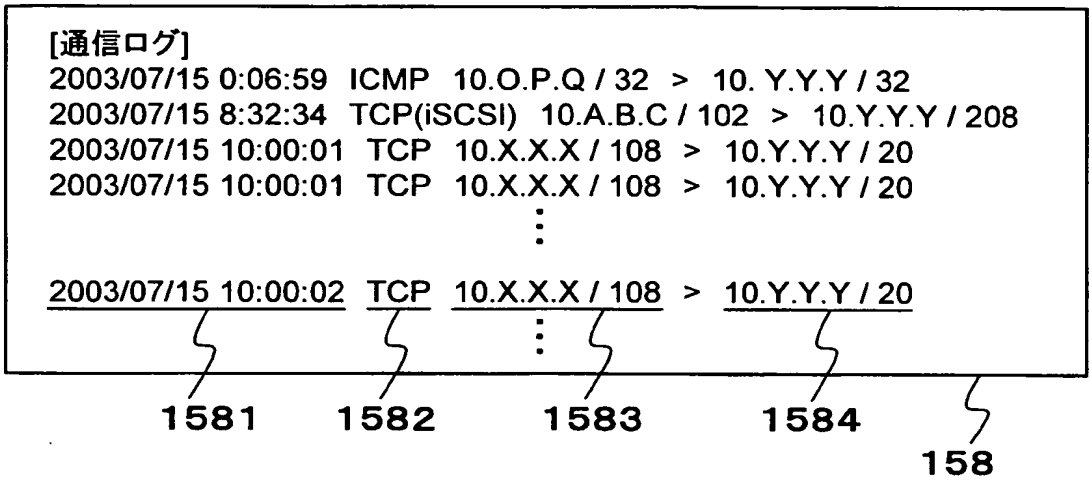
【図４】

図4


122a
122b
判定対象通信比
閾値
1221
非iSCSIパケット通信量(/S) / 全通信量(/S)
50%以上
1222
不許可iSCSIパケット通信量(/S) / iSCSIパケット全通信量(/S)
30%以上
1223
許可iSCSIパケット通信量(/S) / 全通信量(/S)
60%以下
122

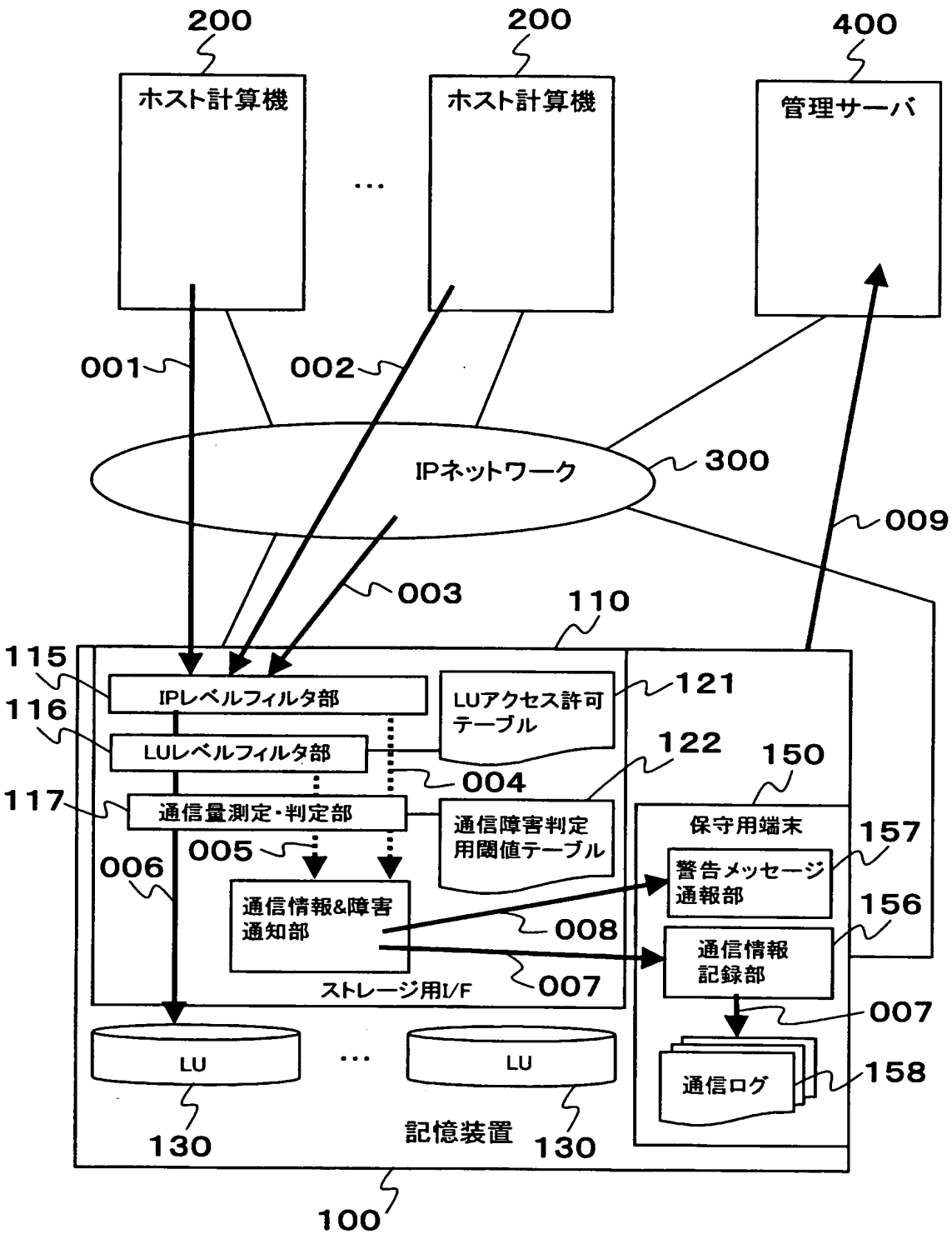
【図５】

図5


[通信ログ]
2003/07/15 0:06:59 ICMP 10.O.P.Q / 32 > 10. Y.Y.Y / 32
2003/07/15 8:32:34 TCP(iSCSI) 10.A.B.C / 102 > 10.Y.Y.Y / 208
2003/07/15 10:00:01 TCP 10.X.X.X / 108 > 10.Y.Y.Y / 20
2003/07/15 10:00:01 TCP 10.X.X.X / 108 > 10.Y.Y.Y / 20
2003/07/15 10:00:02 TCP 10.X.X.X / 108 > 10.Y.Y.Y / 20
1581
1582
1583
1584
158

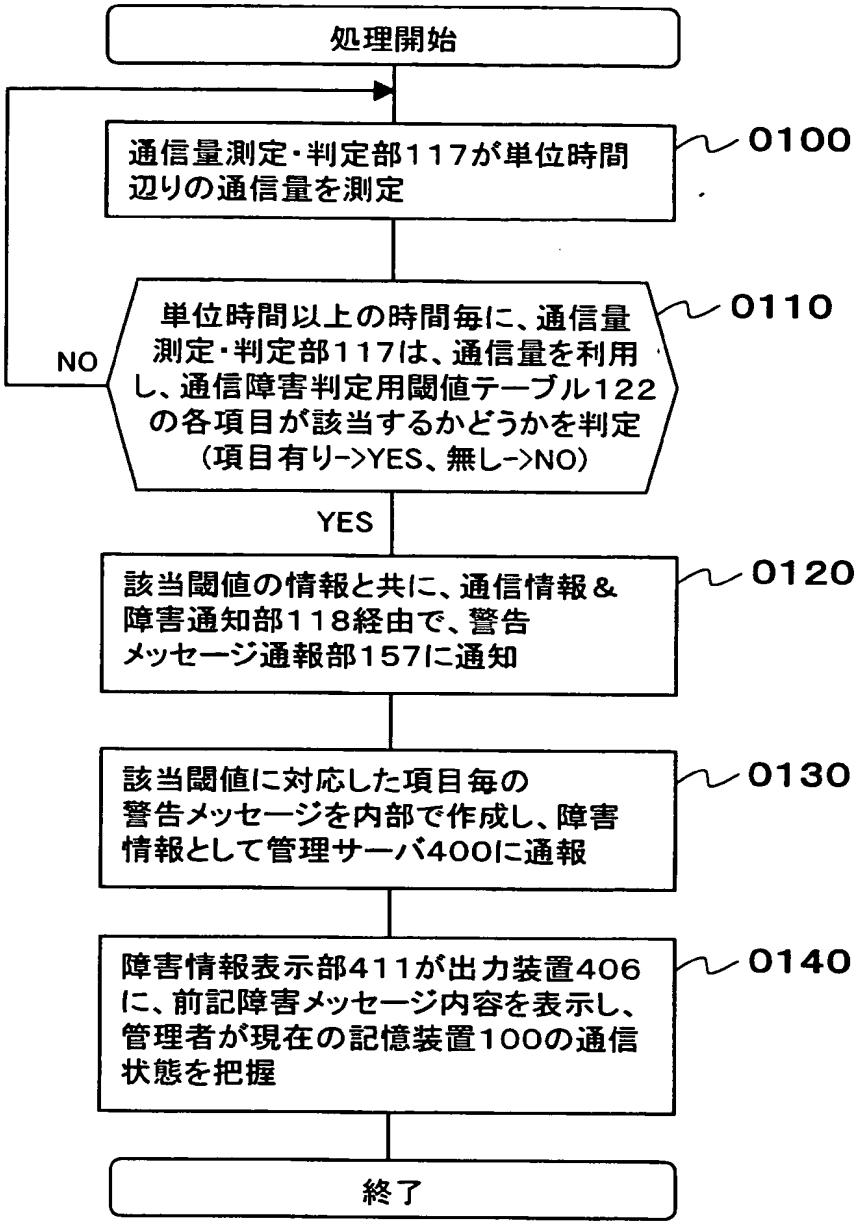
【図６】

図6


200
200
400
ホスト計算機
ホスト計算機
管理サーバ
001
002
IPネットワーク
300
009
003
110
115
116
117
IPレベルフィルタ部
LUレベルフィルタ部
通信量測定・判定部
LUアクセス許可テーブル
121
122
004
通信障害判定用閾値テーブル
150
保守用端末
157
警告メッセージ通報部
156
通信情報記録部
005
006
通信情報&障害通知部
008
007
ストレージ用I/F
007
LU
LU
通信ログ
158
130
記憶装置
130
100

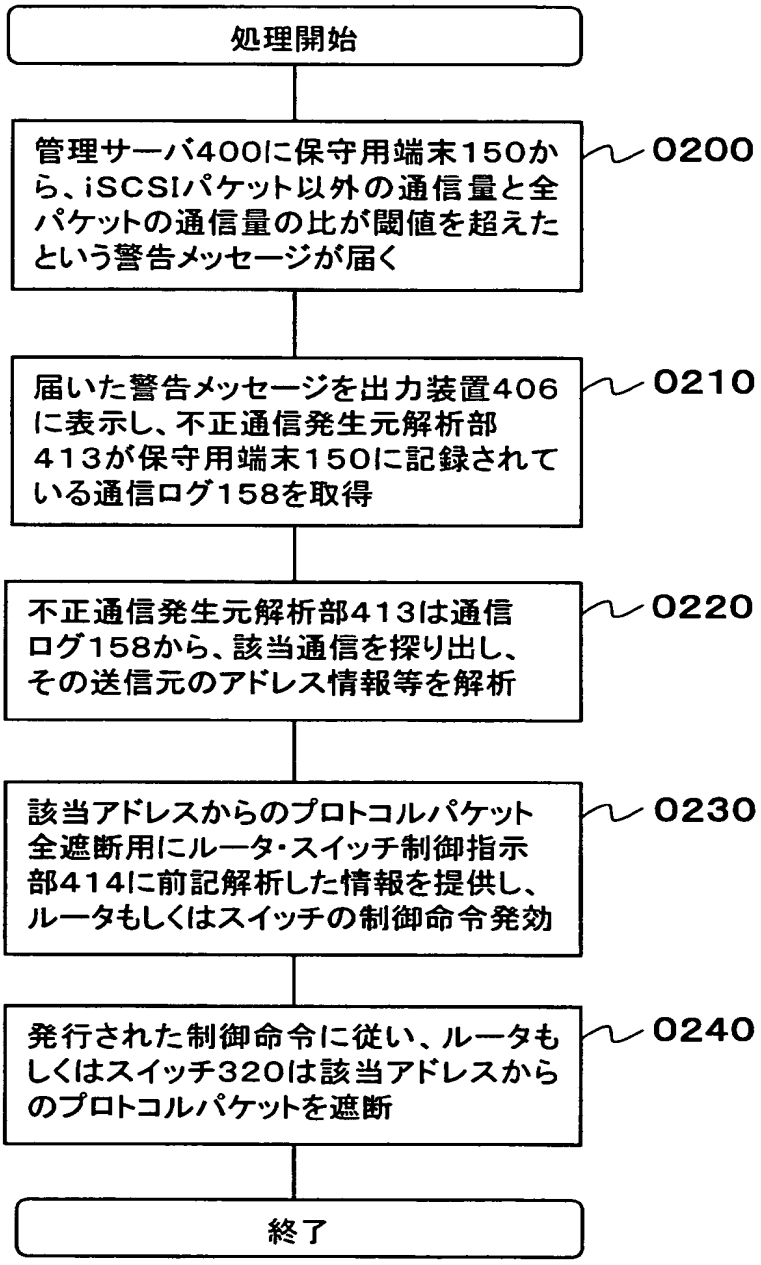
【図７】

図7


処理開始
通信量測定・判定部117が単位時間辺りの通信量を測定
0100
単位時間以上の時間毎に、通信量測定・判定部117は、通信量を利用し、通信障害判定用閾値テーブル122の各項目が該当するかどうかを判定（項目有り->YES、無し->NO）
0110
NO
YES
該当閾値の情報と共に、通信情報＆障害通知部118経由で、警告メッセージ通報部157に通知
0120
該当閾値に対応した項目毎の警告メッセージを内部で作成し、障害情報として管理サーバ400に通報
0130
障害情報表示部411が出力装置406に、前記障害メッセージ内容を表示し、管理者が現在の記憶装置100の通信状態を把握
0140
終了

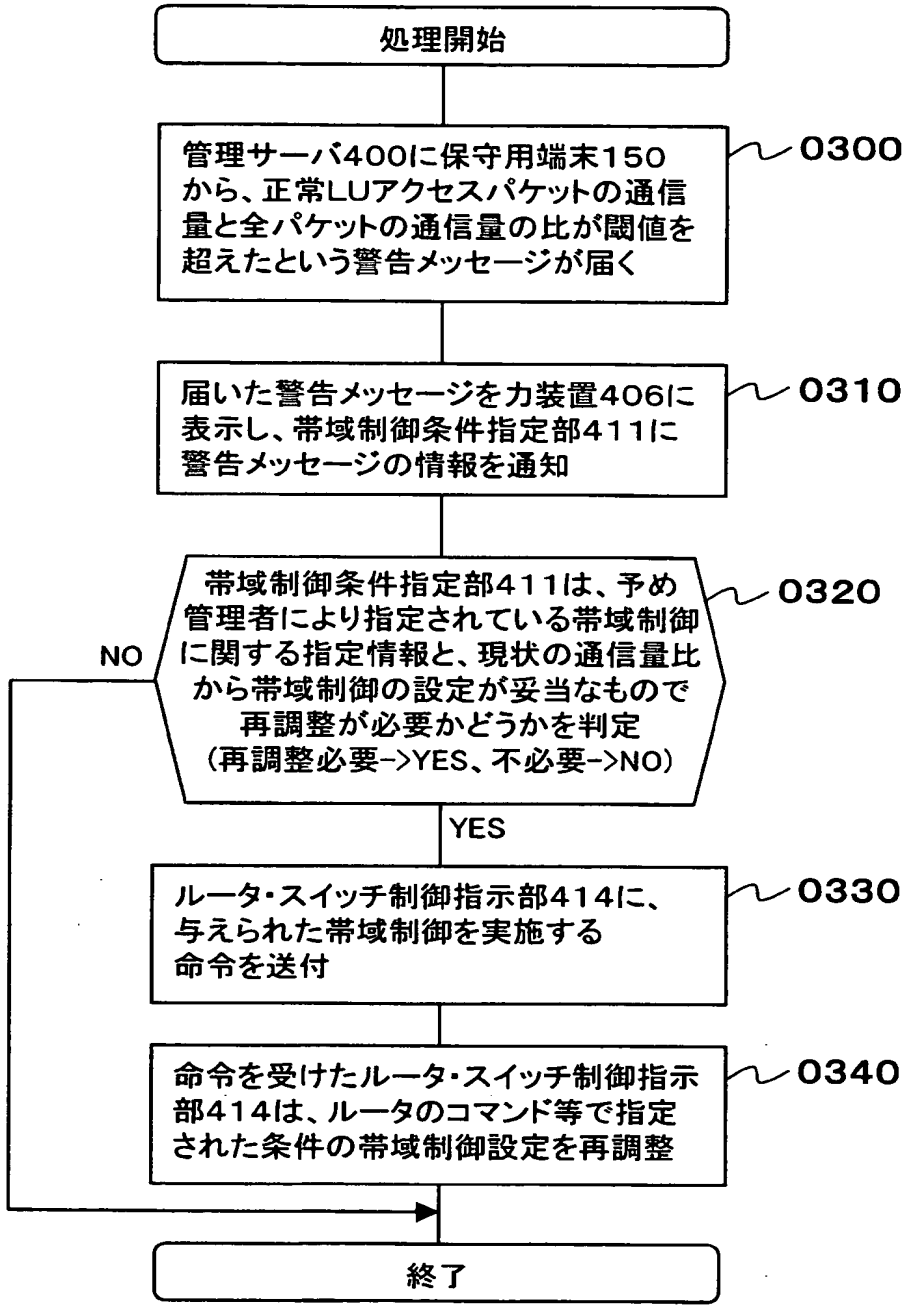
【図８】

図8


処理開始
管理サーバ400に保守用端末150から、iSCSIパケット以外の通信量と全パケットの通信量の比が閾値を超えたという警告メッセージが届く
0200
届いた警告メッセージを出力装置406に表示し、不正通信発生元解析部413が保守用端末150に記録されている通信ログ158を取得
0210
不正通信発生元解析部413は通信ログ158から、該当通信を探り出し、その送信元のアドレス情報等を解析
0220
該当アドレスからのプロトコルパケット全遮断用にルータ・スイッチ制御指示部414に前記解析した情報を提供し、ルータもしくはスイッチの制御命令発効
0230
発行された制御命令に従い、ルータもしくはスイッチ320は該当アドレスからのプロトコルパケットを遮断
0240
終了

【図９】

図9


処理開始
管理サーバ400に保守用端末150から、正常LUアクセスパケットの通信量と全パケットの通信量の比が閾値を超えたという警告メッセージが届く
0300
届いた警告メッセージを力装置406に表示し、帯域制御条件指定部411に警告メッセージの情報を通知
0310
帯域制御条件指定部411は、予め管理者により指定されている帯域制御に関する指定情報と、現状の通信量比から帯域制御の設定が妥当なもので再調整が必要かどうかを判定（再調整必要->YES、不必要->NO）
0320
NO
YES
ルータ・スイッチ制御指示部414に、与えられた帯域制御を実施する命令を送付
0330
命令を受けたルータ・スイッチ制御指示部414は、ルータのコマンド等で指定された条件の帯域制御設定を再調整
0340
終了

【書類名】要約書
【要約】
【課題】
ＩＰネットワークに接続された記憶装置において、不正なパケットを排除することによりセキュリティを高めるとともに、記憶装置の論理ユニットへの通信性能を維持確保する。
【解決手段】
記憶装置内に、ｉＳＣＳＩパケット以外のパケットをフィルタリングする機能を備える。当該機能を通過したもののみ、論理ユニットへのアクセスの可否をフィルタリングする。
また、受信した全てのパケット、および、上記の２つのフィルタリング機能で振り分けられた各パケットごとの通信量を測定するとともに上記フィルタリングで廃棄扱いとなったパケットの通信ログを記録する。これらの情報を用いて、不正通信の遮断処理、正常通信のための帯域確保などの制御を行う。
【選択図】図２

特願２００３－３８９４７５

出　願　人　履　歴　情　報

識別番号　［０００００５１０８］

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所